14-42
ACLU v. Clapper

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2014

(Argued: September 2, 2014 Decided: May 7, 2015)

Docket No. 14-42-cv

AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, NEW YORK CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellants,

— v. —

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence, MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service, ASHTON B. CARTER, in his official capacity as Secretary of Defense, LORETTA E. LYNCH, in her official capacity as Attorney General of the United States, and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants-Appellees.[*]

[*] The Clerk of Court is respectfully directed to amend the official caption in this case to conform with the caption above. See Fed. R. App. P. 43(c)(2).

B e f o r e:

SACK and LYNCH , *Circuit Judges*, and BRODERICK, *District Judge*.[**]

Plaintiffs-appellants American Civil Liberties Union and American Civil Liberties Union Foundation, and New York Civil Liberties Union and New York Civil Liberties Union Foundation, appeal from a decision of the United States District Court for the Southern District of New York (William H. Pauley, III, *Judge*) granting defendants-appellees' motion to dismiss and denying plaintiffs-appellants' request for a preliminary injunction. The district court held that § 215 of the PATRIOT Act impliedly precludes judicial review; that plaintiffs-appellants' statutory claims regarding the scope of § 215 would in any event fail on the merits; and that § 215 does not violate the Fourth or First Amendments to the United States Constitution. We disagree in part, and hold that § 215 and the statutory scheme to which it relates do not preclude judicial review, and that the bulk telephone metadata program is not authorized by § 215. We therefore

[**] The Honorable Vernon S. Broderick, of the United States District Court for the Southern District of New York, sitting by designation.

VACATE the judgment of the district court and REMAND for further proceedings consistent with this opinion.

VACATED AND REMANDED.

Robert D. Sack, *Circuit Judge*, concurs in the opinion of the Court and files a separate concurring opinion.

ALEXANDER ABDO, American Civil Liberties Union Foundation (Jameel Jaffer, Patrick Toomey, Brett Max Kaufman, Catherine Crump, American Civil Liberties Union Foundation, New York, NY; Christopher T. Dunn, Arthur N. Eisenburg, New York Civil Liberties Union Foundation, New York, NY, *on the brief*), New York, NY, *for Plaintiffs-Appellants*.

STUART F. DELERY, Assistant Attorney General, Civil Division, United States Department of Justice (Douglas N. Letter, H. Thomas Byron III, Henry C. Whitaker, Appellate Staff, Civil Division, United States Department of Justice, Washington, DC; Preet Bharara, United States Attorney for the Southern District of New York, New York, NY; David S. Jones, John D. Clopper, Emily E. Daughtry, Assistant United States Attorneys, New York, NY, *on the brief*), Washington, D.C., *for Defendants-Appellees*.

Laura K. Donohue, Georgetown University Law Center, Washington DC, Erwin Chemerinsky, University of California, Irvine School of Law, Irvine, CA, *for Amici Curiae Former Members of the Church Committee and Law Professors in Support of Plaintiffs-Appellants*.

Charles S. Sims, Proskauer Rose LLP, New York, NY, *for Amici Curiae Senator Ron Wyden, Senator Mark Udall, and Senator Martin Heinrich in Support of Plaintiffs-Appellants*.

Cindy Cohn, Mark Rumold, Andrew Crocker, Electronic Frontier Foundation, San Francisco, CA, *for Amici Curiae Experts in Computer and Data Science in Support of Appellants and Reversal*.

John W. Whitehead, Douglas R. McKusick, The Rutherford Institute, Charlottesville, Virginia, Daniel L. Ackman, Law Office of Daniel Ackman, New York, NY, *for Amicus Curiae The Rutherford Institute in Support of Appellants and Reversal*.

Edward J. Davis, Linda Steinman, Lacy H. Koonce, III, Davis Wright Tremaine LLP, New York, NY, *for Amicus Curiae PEN American Center, Inc., in Support of Appellants.*

John Frazer, Law Office of John Frazer, PLLC, Fairfax, VA, *for Amicus Curiae National Rifle Association of America, Inc., in Support of Plaintiffs-Appellants and Supporting Reversal*.

Jonathan Hafetz, Association of the Bar of the City of New York, Gary D. Sesser, Stephen L. Kass, Michael Shapiro, Laura A. Zaccone, Carter Ledyard & Milburn LLP, New York, NY, *for Amicus Curiae Association of the Bar of the City of New York Supporting Plaintiffs-Appellants' Brief.*

GERARD E. LYNCH, *Circuit Judge*:

This appeal concerns the legality of the bulk telephone metadata collection program (the "telephone metadata program"), under which the National Security Agency ("NSA") collects in bulk "on an ongoing daily basis" the metadata associated with telephone calls made by and to Americans, and aggregates those metadata into a repository or data bank that can later be queried. Appellants

challenge the program on statutory and constitutional grounds. Because we find that the program exceeds the scope of what Congress has authorized, we vacate the decision below dismissing the complaint without reaching appellants' constitutional arguments. We affirm the district court's denial of appellants' request for a preliminary injunction.

BACKGROUND

In the early 1970s, in a climate not altogether unlike today's, the intelligence-gathering and surveillance activities of the NSA, the FBI, and the CIA came under public scrutiny. The Supreme Court struck down certain warrantless surveillance procedures that the government had argued were lawful as an exercise of the President's power to protect national security, remarking on "the inherent vagueness of the domestic security concept [and] the necessarily broad and continuing nature of intelligence gathering." United States v. U.S. Dist. Court for the E. Dist. of Mich. (Keith), 407 U.S. 297, 320 (1972). In response to that decision and to allegations that those agencies were abusing their power in order to spy on Americans, the Senate established the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee") to investigate whether the intelligence agencies had engaged in

unlawful behavior and whether legislation was necessary to govern their activities. The Church Committee expressed concerns that the privacy rights of U.S. citizens had been violated by activities that had been conducted under the rubric of foreign intelligence collection.

The findings of the Church Committee, along with the Supreme Court's decision in Keith and the allegations of abuse by the intelligence agencies, prompted Congress in 1978 to enact comprehensive legislation aimed at curtailing abuses and delineating the procedures to be employed in conducting surveillance in foreign intelligence investigations. That legislation, the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801 et seq.), established a special court, the Foreign Intelligence Surveillance Court ("FISC"), to review the government's applications for orders permitting electronic surveillance. See 50 U.S.C. § 1803. Unlike ordinary Article III courts, the FISC conducts its usually ex parte proceedings in secret; its decisions are not, in the ordinary course, disseminated publicly. Id. § 1803(c).

We are faced today with a controversy similar to that which led to the Keith decision and the enactment of FISA. We must confront the question

whether a surveillance program that the government has put in place to protect national security is lawful. That program involves the bulk collection by the government of telephone metadata created by telephone companies in the normal course of their business but now explicitly required by the government to be turned over in bulk on an ongoing basis. As in the 1970s, the revelation of this program has generated considerable public attention and concern about the intrusion of government into private matters. As in that era, as well, the nation faces serious threats to national security, including the threat of foreign-generated acts of terrorism against the United States. Now, as then, Congress is tasked in the first instance with achieving the right balance between these often-competing concerns. To do so, Congress has amended FISA, most significantly, after the terrorist attacks of September 11, 2001, in the PATRIOT Act. See USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). The government argues that § 215 of that Act authorizes the telephone metadata program. See id. § 215, 115 Stat. at 287 (codified as amended at 50 U.S.C. § 1861).

I. Telephone Metadata

Before proceeding to explore the details of § 215 of the PATRIOT Act, we pause to define "telephone metadata," in order to clarify the type of information

that the government argues § 215 authorizes it to collect in bulk. Unlike what is gleaned from the more traditional investigative practice of wiretapping, telephone metadata do not include the voice content of telephone conversations. Rather, they include details about telephone calls, including, for example, the length of a call, the phone number from which the call was made, and the phone number called. Metadata can also reveal the user or device making or receiving a call through unique "identity numbers" associated with the equipment (although the government maintains that the information collected does not include information about the identities or names of individuals), and provide information about the routing of a call through the telephone network, which can sometimes (although not always) convey information about a caller's general location. According to the government, the metadata it collects do not include cell site locational information, which provides a more precise indication of a caller's location than call-routing information does.

That telephone metadata do not directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data. Appellants and amici take pains to emphasize the startling amount of detailed information metadata can reveal –

"information that could traditionally only be obtained by examining the contents of communications" and that is therefore "often a proxy for content." Joint App'x 50 (Declaration of Professor Edward W. Felten). For example, a call to a single-purpose telephone number such as a "hotline" might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships.[1]

---

[1] A report of a recent study in *Science* magazine revealed how much information can be gleaned from credit card metadata. In the study, which used three months of anonymous credit card records for 1.1 million people, scientists were able to reidentify 90% of the individuals where they had only four additional "spatiotemporal points" of information – for example, information that an individual went to one particular store on four specific days. Such information could be gathered from sources as accessible as a "tweet" from that individual. Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex "Sandy" Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, Science, Jan. 30, 2015, at 536. The study's authors concluded that, in the context of most large-scale metadata sets, it would not be difficult to reidentify individuals even if the data were anonymized. Id. at 539. While credit card data differ in important ways from telephone data, the study illustrates the ways in which metadata can be used by sophisticated investigators to deduce significant private information about individuals.

We recognize that metadata exist in more traditional formats, too, and that law enforcement and others have always been able to utilize metadata for investigative purposes. For example, just as telephone metadata may reveal the charitable organizations that an individual supports, observation of the outside of an envelope sent at the end of the year through the United States Postal Service to such an organization might well permit similar inferences, without requiring an examination of the envelope's contents. But the structured format of telephone and other technology-related metadata, and the vast new technological capacity for large-scale and automated review and analysis, distinguish the type of metadata at issue here from more traditional forms. The more metadata the government collects and analyzes, furthermore, the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals. Finally, as appellants and amici point out, in today's technologically based world, it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his ordinary affairs.

II. Section 215

The original version of § 215, which pre-dated the PATRIOT Act, allowed

the Director of the FBI or his designee to obtain orders from the FISC authorizing common carriers, among others, to provide to the government certain business records for the purpose of foreign intelligence and international terrorism investigations where there existed "specific and articulable facts giving reason to believe that the person to whom the records pertain [wa]s a foreign power or an agent of a foreign power." That provision was enacted in 1998 as an amendment to FISA. See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410-11 (1998). The PATRIOT Act substantially revised § 215 to provide for the production not only of "business records" but also of "any tangible things," and to eliminate the restrictions on the types of businesses such orders can reach. See USA PATRIOT ACT of 2001, Pub. L. No. 107-56, § 215. As subsequently amended by successor bills to the PATRIOT Act, the current version of § 215 allows the Director of the FBI or his designee to

> make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

50 U.S.C. § 1861(a)(1). In its current form, the provision requires such an application to include

> a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Id. § 1861(b)(2)(A). Such an order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." Id. § 1861(c)(2)(D). Finally, the statute requires the Attorney General to "adopt specific minimization procedures governing the retention and dissemination by the [FBI] of any tangible things, or information therein, received by the [FBI] in response to an order under this subchapter." Id. § 1861(g)(1). Because § 215 contained a "sunset" provision from its inception, originally terminating its authority on December 31, 2005, it has required subsequent renewal. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 224, 115 Stat. at 295.

Congress has renewed § 215 seven times, most recently in 2011, at which time it was amended to expire on June 1, 2015. See PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

III. The Telephone Metadata Program

Americans first learned about the telephone metadata program that appellants now challenge on June 5, 2013, when the British newspaper *The Guardian* published a FISC order leaked by former government contractor Edward Snowden. The order directed Verizon Business Network Services, Inc. ("Verizon"), a telephone company, to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc., ex rel. MCI Commc'n Servs., Inc., d/b/a Verizon Bus. Servs. ("Verizon Secondary Order"), No. BR 13-80, slip op. at 2 (F.I.S.C. Apr. 25, 2013). The order thus requires Verizon to produce call detail records, every day, on *all* telephone calls made through its systems or using its services where one or both ends of the call are located in the United States.

After the order was published, the government acknowledged that it was part of a broader program of bulk collection of telephone metadata from other telecommunications providers carried out pursuant to § 215. It is now undisputed that the government has been collecting telephone metadata information in bulk under § 215 since at least May 2006, when the FISC first authorized it to do so in a "Primary Order" describing the "tangible things" to be produced as "all call-detail records or 'telephony metadata' created by [redacted] . . . , includ[ing] comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number[s], communications device identifier[s], etc.), trunk identifier, and time and duration of call." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted] ("2006 Primary Order"), No. BR 06-05, slip op. at 2 (F.I.S.C. May 24, 2006), http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

That order specified that the items were to be produced to the NSA; that there were "reasonable grounds to believe the tangible things sought [were] relevant to authorized investigations . . . to protect against international

terrorism"; and that the items sought "could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." Id. at 3. The order required its recipient, upon receiving the "appropriate secondary order,"[2] to "continue production on an ongoing daily basis . . . for the duration of th[e] order" and contemplated creation of a "data archive" that would only be accessed "when NSA has identified a known telephone number for which . . . there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [Redacted]"– presumably, with terrorist activity or a specific terrorist organization. Id. at 4-5. The order also states that the NSA "exclusively will operate" the network on which the metadata are stored and processed. Id. at 5.

The government has disclosed additional FISC orders reauthorizing the program. FISC orders must be renewed every 90 days, and the program has therefore been renewed 41 times since May 2006. Most recently, the program

[2] The order published in *The Guardian* and served on Verizon was one such "Secondary Order."

was reauthorized by the FISC on February 26, 2015; that authorization expires on June 1, 2015. See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 15-24 (F.I.S.C. Feb. 26, 2015), http://www.dni.gov/files/documents/0311/BR%2015-24%20Primary%20Order%20-%20Redacted.pdf.

The government disputes appellants' characterization of the program as collecting "virtually all telephony metadata" associated with calls made or received in the United States, but declines to elaborate on the scope of the program or specify how the program falls short of that description. It is unclear, however, in what way appellants' characterization of the program can be faulted. On its face, the Verizon order requires the production of "*all* call detail records or 'telephony metadata'" relating to Verizon communications within the United States or between the United States and abroad. Verizon Secondary Order 2 (emphasis added). The Verizon order and the Primary Order described above reveal that the metadata collected include "comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment

Identity (IMEI) number, etc.), trunk identifier,[3] telephone calling card numbers, and time and duration of call." Verizon Secondary Order 2; see also 2006 Primary Order 2. The government does not suggest that Verizon is the only telephone service provider subject to such an order; indeed, it does not seriously dispute appellants' contention that all significant service providers in the United States are subject to similar orders.

The government explains that it uses the bulk metadata collected pursuant to these orders by making "queries" using metadata "identifiers" (also referred to as "selectors"), or particular phone numbers that it believes, based on "reasonable articulable suspicion," to be associated with a foreign terrorist organization. Joint App'x 264 (Declaration of Teresa H. Shea). The identifier is used as a "seed" to search across the government's database; the search results yield phone numbers, and the metadata associated with them, that have been in contact with the seed. Id. That step is referred to as the first "hop." The NSA can then also search for the numbers, and associated metadata, that have been in contact with the numbers resulting from the first search – conducting a second

[3] A "trunk identifier" provides information regarding how a call is routed through the telephone network, revealing general information about the parties' locations.

"hop." Id. at 265. Until recently, the program allowed for another iteration of the process, such that a third "hop" could be conducted, sweeping in results that include the metadata of, essentially, the contacts of contacts of contacts of the original "seed." Id. The government asserts that it does not conduct any general "browsing" of the data. Id. at 263-65.

Section 215 requires that the Attorney General adopt "specific minimization procedures governing the retention and dissemination by the [government] of [information] received . . . in response to an order under this subchapter." 50 U.S.C. § 1861(g)(1). The procedures that have been adopted include the requirement that the NSA store the metadata within secure networks; that the metadata not be accessed for any purpose other than what is allowed under the FISC order; that the results of queries not be disseminated outside the NSA except in accordance with the minimization and dissemination requirements of NSA procedures; and that the relevant personnel receive comprehensive training on the minimization procedures and technical controls. Joint App'x 267-69. And as the government points out, the program is subject to oversight by the Department of Justice, the FISC, and Congress. Id. at 269. The minimization procedures require audits and reviews of the program by the

NSA's legal and oversight offices, the Office of the Inspector General, attorneys from the Department of Justice's National Security Division, and the Office of the Director of National Intelligence. Id. The FISC orders that created the program require the NSA to provide periodic reports to the FISC. Id. at 141. In the event of failures of compliance, reports must be made to the FISC, and, where those failures are significant, to the Intelligence and Judiciary Committees of both houses of Congress. Id. at 269. FISA itself also imposes a system of Congressional oversight, requiring periodic reports on the program from the Attorney General to the House and Senate Intelligence and Judiciary Committees. See 50 U.S.C. §§ 1862, 1871.

Since the existence of the telephone metadata program became public, a number of developments have altered the landscape, at least to some degree, within which we analyze the program. Among the most notable are modifications to the telephone metadata program announced by President Obama in January 2014. President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. The two immediate modifications that the President ordered, which were subsequently

incorporated in a FISC order sought by government motion, (1) limited the number of "hops" that can be searched to two, rather than three, and (2) required that a FISC judge find that the reasonable articulable suspicion standard has been satisfied before a seed can be queried, rather than (as had previously been the case) allowing designated NSA officials to determine for themselves whether such suspicion existed. Id. Both limitations were approved by the FISC in a February 5, 2014 FISC order. In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR-14-01 (F.I.S.C. Feb. 5, 2014), http://www.uscourts.gov/uscourts/courts/fisc/br14-01-order.pdf. These modifications were based in part on the recommendations of the Review Group on Intelligence and Communications Technologies established by the President. See President's Review Grp. on Intelligence and Commc'ns Techs., Liberty and Security in a Changing World: Rep. and Recommendations of the President's Review Grp. on Intelligence and Commc'ns Techs. (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. The Review Group also recommended that the system be modified such that a third party or the private carriers, rather than the government, collect and

retain the bulk metadata. That recommendation, however, has so far not been adopted.

In addition to that group, the Privacy and Civil Liberties Oversight Board ("PCLOB") published a detailed report on the program. The PCLOB is a bipartisan agency within the executive branch that was established in 2007, pursuant to a recommendation from the National Commission on Terrorist Attacks Upon the United States (the "9/11 Commission," established after the September 11, 2001 terrorist attacks to prepare an account of the circumstances surrounding the attacks), in order to monitor the actions taken by the government to protect the nation from terrorism and to ensure that they are appropriately balanced against the need to protect privacy and civil liberties. See Implementing Recommendations of the 9/11 Comm'n Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007). The PCLOB concluded that the program was inconsistent with § 215, violated the Electronic Communications Privacy Act, and implicated privacy and First Amendment concerns. See Privacy and Civil Liberties Oversight Board, Rep. on the Tel. Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Jan. 23, 2014) ("PCLOB Report"),

https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Legislation aimed at incorporating stronger protections of individual liberties into the telephone metadata program in a variety of ways (or eliminating it altogether) was introduced in both the House and the Senate during the 113th Congress. See USA FREEDOM Act, H.R. 3361, 113th Cong. (2014); USA FREEDOM Act, S. 2685, 113th Cong. (2014). A modified version of H.R. 3361, which lost the backing of some of the bill's original supporters because it failed to end bulk collection, nevertheless passed the House in May 2014. USA FREEDOM Act, H.R. 3361, 113th Cong. (2014). In November 2014, however, a motion to invoke cloture on the Senate's version of the bill – relatively more robust in terms of privacy protections – failed by a vote of 58-42, thereby preventing the bill from coming up for a vote in the Senate despite the desire of 58 senators to proceed to a vote on the measure. USA FREEDOM Act, S. 2685, 113th Cong. (2014). The current Congress is likewise considering bills aimed at modifying § 215; a bill that would place the bulk metadata collected into the hands of telecommunications providers, to be accessed by the government only with FISC authorization, has been introduced in both the House and the Senate in

recent weeks. See USA FREEDOM Act of 2015, H.R. 2048/S. 1123, 114th Cong. (2015). On April 30, 2015, the bill passed the House Judiciary Committee. See USA FREEDOM Act of 2015, H.R. 2048, 114th Cong. (2015). A vote from the full House on the bill is expected later this month.

Finally, the program has come under scrutiny by Article III courts other than the FISC. In addition to this case, similar cases have been filed around the country challenging the government's bulk collection of telephone metadata. See, e.g., Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), No. 14-35555 (9th Cir. argued Dec. 8, 2014); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), No. 14-5004 (D.C. Cir. argued Nov. 4, 2014).

IV. Procedural History

On June 11, 2013, the American Civil Liberties Union and American Civil Liberties Union Foundation (collectively, "ACLU") and the New York Civil Liberties Union and New York Civil Liberties Union Foundation (collectively, "NYCLU") – current and former Verizon customers, respectively – sued the government officials responsible for administering the telephone metadata program, challenging the program on both statutory and constitutional grounds and seeking declaratory and injunctive relief. The complaint asks the court to

declare that the telephone metadata program exceeds the authority granted by § 215, and also violates the First and Fourth Amendments to the U.S. Constitution. It asks the court to permanently enjoin defendants from continuing the program, and to order defendants to "purge from their possession all of the call records of [p]laintiffs' communications" collected in accordance with the program. Joint App'x 27.

On August 26, 2013, plaintiffs moved for a preliminary injunction barring defendants from collecting their call records under the program, requiring defendants to quarantine all of the call records they had already collected, and prohibiting defendants from using their records to perform queries on any phone number or other identifier associated with plaintiffs. On the same date, the government moved to dismiss the complaint.

On December 27, 2013, the district court granted the government's motion to dismiss and denied plaintiffs' motion for a preliminary injunction. See ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013). Plaintiffs now appeal that decision.

DISCUSSION

We review de novo a district court's grant of a motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Klein & Co. Futures, Inc. v. Bd. of Trade of City of New York, 464 F.3d 255, 259 (2d Cir. 2006); see also Lotes Co., Ltd. v. Hon Hai Precision Indus. Co., 753 F.3d 395, 403 (2d Cir. 2014). We review a district court's denial of a preliminary injunction for abuse of discretion, see Cent. Rabbinical Cong. of U.S. & Canada v. N.Y.C. Dep't of Health & Mental Hygiene, 763 F.3d 183, 192 (2d Cir. 2014), which occurs when the court's decision either "rests on an error of law . . . or a clearly erroneous factual finding, or . . . its decision – though not necessarily the product of a legal error or a clearly erroneous factual finding – cannot be located within the range of permissible decisions," Vincenty v. Bloomberg, 476 F.3d 74, 83 (2d Cir. 2007).

I. Standing

The district court ruled that appellants had standing to bring this case. Clapper, 959 F. Supp. 2d at 738. The government argues that the district court's ruling was erroneous, contending that appellants lack standing because they have not demonstrated that any of the metadata associated with them have been or will be actually reviewed by the government, and have not otherwise

identified an injury that is sufficiently concrete or imminent to confer standing. We recognize that "'[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.'" Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013), quoting DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (alteration in original). In order to meet that requirement, plaintiffs must, among other things, establish that they have standing to sue. Raines v. Byrd, 521 U.S. 811, 818 (1997). "Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010); see also Amnesty Int'l, 133 S. Ct. at 1147 (collecting cases). The Supreme Court has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." Amnesty Int'l, 133 S. Ct. at 1147, quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (emphasis in original). We remain mindful that the "'standing inquiry has been especially rigorous when reaching the merits of [a] dispute would force us to decide whether an action taken by one of the

other two branches of the Federal Government was unconstitutional'" and "in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." Id., quoting Raines, 521 U.S. at 819-20.

Appellants in this case have, despite those substantial hurdles, established standing to sue, as the district court correctly held. Appellants here need not speculate that the government has collected, or may in the future collect, their call records. To the contrary, the government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program. Nor has the government disputed that claim. It argues instead that any alleged injuries here depend on the government's *reviewing* the information collected, and that appellants have not shown anything more than a "speculative prospect that their telephone numbers would ever be used as a selector to query, or be included in the results of queries of, the telephony metadata." Appellees' Br. 22.

But the government's argument misapprehends what is required to establish standing in a case such as this one. Appellants challenge the telephone metadata program as a whole, alleging injury from the very collection of their

telephone metadata. And, as the district court observed, it is not disputed that the government collected telephone metadata associated with the appellants' telephone calls. The Fourth Amendment protects against unreasonable searches *and seizures*. Appellants contend that the collection of their metadata exceeds the scope of what is authorized by § 215 and constitutes a Fourth Amendment search. We think such collection is more appropriately challenged, at least from a standing perspective, as a seizure rather than as a search. Whether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them. "[A] violation of the [Fourth] Amendment is fully accomplished at the time of an unreasonable governmental intrusion." United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (internal quotation marks omitted). If the telephone metadata program is unlawful, appellants have suffered a concrete and particularized injury fairly traceable to the challenged program and redressable by a favorable ruling.

Amnesty International does not hold otherwise. There, the Supreme Court, reversing our decision, held that respondents had not established standing because they could not show that the government was surveilling them, or that

such surveillance was "certainly impending." 131 S. Ct. at 1148-1150. Instead, the Supreme Court stated that respondents' standing arguments were based on a "speculative chain of possibilities" that required that: respondents' foreign contacts be targeted for surveillance; the surveillance be conducted pursuant to the statute challenged, rather than under some other authority; the FISC approve the surveillance; the government actually intercept the communications of the foreign contacts; and among those intercepted communications be those involving respondents. Id. Because respondents' injury relied on that chain of events actually transpiring, the Court held that the alleged injury was not "fairly traceable" to the statute being challenged. Id. at 1150. As to costs incurred by respondents to avoid surveillance, the Court characterized those costs as "a product of their fear of surveillance" insufficient to confer standing. Id. at 1152.

Here, appellants' alleged injury requires no speculation whatsoever as to how events will unfold under § 215 – appellants' records (among those of numerous others) have been targeted for seizure by the government; the government has used the challenged statute to effect that seizure; the orders have been approved by the FISC; and the records have been collected. Amnesty International's "speculative chain of possibilities" is, in this context, a reality.

That case in no way suggested that such data would need to be reviewed or analyzed in order for respondents to suffer injury.

The government also takes issue with the district court's reliance on Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir. 2011). In Amidax, we held that plaintiffs had not established standing to challenge the government's acquisition of financial records from SWIFT, a messaging service that routes financial transactions, via administrative subpoenas issued by the Office of Foreign Asset Control. Id. at 148-49. Because there was insufficient support for the allegation that Amidax's own records were among those handed over to the government, we held that Amidax had not alleged a plausible injury in fact. Id. That case, too, differs from the case at bar, where appellants have presented evidence that their data *are* being collected. To the extent Amidax speaks to the circumstances presented by this case, it supports, albeit in dictum, appellants' position. We noted in Amidax that "[t]o establish an injury in fact – and thus, a personal stake in this litigation – [Amidax] need only establish that its information was obtained by the government." Id. at 147 (second alteration in original). There, too, we viewed the collection of the data in question, if it had in

fact occurred, as an injury sufficient to confer standing, without considering whether such data were likely to be reviewed.

Finally, the government admits that, when it queries its database, its computers search all of the material stored in the database in order to identify records that match the search term. In doing so, it necessarily searches appellants' records electronically, even if such a search does not return appellants' records for close review by a human agent. There is no question that an equivalent manual review of the records, in search of connections to a suspect person or telephone, would confer standing even on the government's analysis. That the search is conducted by a machine might lessen the intrusion, but does not deprive appellants of standing to object to the collection and review of their data.

Appellants likewise have standing to assert a First Amendment violation. Appellants contend that their First Amendment associational rights are being violated, both directly and through a "chilling effect" on clients and donors. The Supreme Court has long recognized that an organization can assert associational privacy rights on behalf of its members, stating that "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in

advocacy may constitute . . . a restraint on freedom of association." NAACP v. Alabama, 357 U.S. 449, 462 (1958). In NAACP, furthermore, the Supreme Court held that the organization "argue[d] . . . appropriately the rights of its members, and that its nexus with them [wa]s sufficient to permit that it act as their representative before this Court." Id. at 458-59. We have similarly stated that a union's "standing to assert the First and Fourteenth Amendment rights of association and privacy of its individual members is beyond dispute." Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 270 (2d Cir. 1981). When the government collects appellants' metadata, appellants' members' interests in keeping their associations and contacts private are implicated, and any potential "chilling effect" is created at that point. Appellants have therefore alleged a concrete, fairly traceable, and redressable injury sufficient to confer standing to assert their First Amendment claims as well.

II. Preclusion and the Administrative Procedure Act

The government next contends that appellants are impliedly precluded from bringing suit to challenge the telephone metadata program on statutory grounds. According to the government, the statutory scheme set out by § 215

limits judicial review of § 215 orders "to the FISC and its specialized mechanism for appellate review," Appellees' Br. 26, and provides for challenges to those orders only by *recipients* of § 215 orders (that is, the communications companies), rather than the targets of such orders, thereby impliedly precluding appellants here from bringing suit in federal court. The government also argues that 18 U.S.C. § 2712 impliedly precludes the relief appellants seek, either independently or in conjunction with the larger statutory framework established by the two provisions.

A. Section 215 and Implied Preclusion

The Administrative Procedure Act ("APA") waives sovereign immunity for suits against the United States for relief other than money damages. Under the APA, "[a] person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof," and can bring suit in an "action in a court of the United States seeking relief other than money damages." 5 U.S.C. § 702. The APA thus establishes a broad right of judicial review of administrative action. The APA does not, however, apply where "statutes preclude judicial review." Id. § 701.

In determining whether judicial review is precluded under a particular statute, we must "begin with the strong presumption that Congress intends judicial review of administrative action. From the beginning 'our cases [have established] that judicial review of a final agency action by an aggrieved person will not be cut off unless there is persuasive reason to believe that such was the purpose of Congress.'" Bowen v. Mich. Acad. of Family Physicians, 476 U.S. 667, 670 (1986), quoting Abbott Labs. v. Gardner, 387 U.S. 136, 140 (1967) (alterations in original). "'[O]nly . . . a showing of clear and convincing evidence of a contrary legislative intent'" can rebut the presumption that Congress intended that an action be subject to judicial review. Bowen, 476 U.S. at 672, quoting Abbott Labs., 387 U.S. at 141. The Supreme Court has emphasized that there is a "heavy burden" on a party that attempts to overcome this presumption. Id. (internal quotation marks omitted).

That burden is, of course, not insurmountable, and "may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent." Block v. Cmty. Nutrition Inst., 467 U.S. 340, 349 (1984). Such an intent must be "fairly discernible in the statutory scheme," id. at 351 (internal quotation marks omitted), looking to the scheme's "structure . . . , its

objectives, its legislative history, and the nature of the administrative action involved," id. at 345. Importantly, "'where substantial doubt about the congressional intent exists, the general presumption favoring judicial review of administrative action is controlling.'" NRDC v. Johnson, 461 F.3d 164, 172 (2d Cir. 2006), quoting Block, 467 U.S. at 351. Implied preclusion of review is thus disfavored.

The government points to no language in § 215, or in FISA or the PATRIOT Act more generally, that excludes actions taken by executive or administrative officials pursuant to its terms from the presumption of judicial review established by the APA. Rather, it argues that the provision of one mechanism for judicial review, at the behest of parties other than those whose privacy may be compromised by the seizure, impliedly precludes review pursuant to the APA by parties thus aggrieved. To understand that argument, we begin by describing the provision for judicial review on which the government relies.

A recipient of a § 215 order may challenge its legality "by filing a petition with the pool" of FISC judges established by the statute. 50 U.S.C. § 1861(f)(2)(A)(i). That decision can then be appealed to the FISA Court of Review. Id. § 1861(f)(3). The statute also provides that "[a]ny production or

nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect." Id. § 1861(f)(2)(D).

According to the government, those provisions establish a limited and detailed framework that evinces Congressional intent to limit judicial review to the method specified. Both the government and the district court point to the Supreme Court's language in Block that "when a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded." Block, 467 U.S. at 349.

But that is not always the case. The Supreme Court has also noted that "if the express provision of judicial review in one section of a long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it would not be much of a presumption at all." Sackett v. EPA, 132 S. Ct. 1367, 1373 (2012). The question remains whether the government has demonstrated by clear and convincing or "discernible" evidence that Congress intended to preclude review in these particular circumstances.

(1) Secrecy

The government's primary argument in support of preclusion is based on the various secrecy provisions that attach to § 215 orders. For example, § 215 states that "[n]o person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section" unless disclosure is necessary to comply with the order; the disclosure is made to an attorney for advice or assistance in connection with the order; or the disclosure is made to others as permitted by the FBI Director or his designee. 50 U.S.C. § 1861(d)(1). And the statute explicitly lays out various supplemental secrecy procedures accompanying the review process, including the requirements that the records of any such proceedings be "maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence," id. § 1861(f)(4); that "[a]ll petitions . . . be filed under seal," id. § 1861(f)(5); and that, in the case of any government submission that may contain classified information, the court review it ex parte and in camera, id. These secrecy measures, the government argues, are evidence that Congress did

not intend that § 215 orders be reviewable in federal court upon suit by an individual whose metadata are collected.

Upon closer analysis, however, that argument fails. The government has pointed to no affirmative evidence, whether "clear and convincing" or "fairly discernible," that suggests that Congress intended to preclude judicial review. Indeed, the government's argument from secrecy suggests that Congress did not contemplate a situation in which targets of § 215 orders would become aware of those orders on anything resembling the scale that they now have. That revelation, of course, came to pass only because of an unprecedented leak of classified information. That Congress may not have anticipated that individuals like appellants, whose communications were targeted by § 215 orders, would become aware of the orders, and thus be in a position to seek judicial review, is not evidence that Congress affirmatively decided to revoke the right to judicial review otherwise provided by the APA in the event the orders *were* publicly revealed.

The government's argument also ignores the fact that, in certain (albeit limited) instances, the statute does indeed contemplate disclosure. If a judge finds that "there is no reason to believe that disclosure may endanger the

national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person," he may grant a petition to modify or set aside a nondisclosure order. 50 U.S.C. § 1861(f)(2)(C)(i). Such a petition could presumably only be brought by a § 215 order recipient, because only the recipient, not the target, would know of the order before such disclosure. But this provision indicates that Congress did not expect that all § 215 orders would remain secret indefinitely and that, by providing for such secrecy, Congress did not intend to preclude targets of § 215 orders, should they happen to learn of them, from bringing suit.

(2) Statutory Scheme

The government also relies heavily on Block in arguing that the statutory scheme as a whole impliedly precludes judicial review. In Block, the Supreme Court considered whether consumers of milk could obtain judicial review of milk market orders, which are issued by the Secretary of Agriculture pursuant to the Agricultural Marketing Agreement Act of 1937 ("AMAA"), codified as amended at 7 U.S.C. § 601 et seq. Those orders set the minimum prices that milk processors (also known as "handlers") must pay to milk producers. The Court

held that, in the context of that statute, the statute's silence as to the ability of milk consumers to challenge milk market orders was sufficient to imply that Congress intended that they be precluded from doing so. 467 U.S. at 347. The government would have us view § 215 as a similarly complex administrative scheme that would clearly be disrupted should targets of the orders be permitted judicial review of them.

But the AMAA and the Court's decision in Block are distinguishable from this case. First, the Court in Block, and in its decisions since Block, has made much of whether a statute has administrative review requirements that would be end-run if the APA provided for ordinary judicial review. In Block, for example, the Court noted that, for a milk market order to become effective, the AMAA requires that: (1) the Secretary of Agriculture conduct a rulemaking proceeding before issuing a milk market order; (2) the public be notified of the proceeding and given an opportunity for comment; (3) a public hearing be held, in which (4) the evidence offered shows that the order will further the statute's policy; and (5) certain percentages of milk handlers and producers vote in favor of the orders. See id. at 342.

Such a scheme is a far cry from what is contemplated by § 215. Section 215 contains no administrative review requirements that would be "end run" if targets of the orders were allowed to obtain judicial review thereof. Indeed, the only express mechanism for any review at all of § 215 orders *is* via judicial review – albeit by the FISC, rather than a federal district court.

Unlike the AMAA, § 215 in no way contemplates a "cooperative venture" that precedes the issuance of orders. Id. at 346. In Block, the Court pointed out that the statute provided for milk handlers and producers – and not consumers – to participate in the adoption of the market orders. See id. Those parties, according to the Court, were the ones who could obtain review of the orders, not the consumers, whom Congress had excluded from the entire process. Section 215, in contrast, does not contemplate ex ante cooperation between, for example, telephone companies and the government in deciding how production orders should be crafted and whether they should be approved. To the contrary, under § 215, the government unilaterally crafts orders that may then be approved or not by the FISC. Unlike in the case of the AMAA, there is no indication that Congress, in drafting § 215, intended that the phone companies be the only party

entitled to obtain judicial review of the orders by providing for them to otherwise participate in the order-issuing process.

Block is further distinguishable because the Court there emphasized the fact that "[h]andlers ha[d] interests similar to those of consumers" and could "therefore be expected to challenge unlawful agency action." Id. at 352. Here, in contrast, the interests and incentives of the recipients of § 215 orders are quite different from those of the orders' targets. As appellants point out, telecommunications companies have little incentive to challenge § 215 orders – first, because they are unlikely to want to antagonize the government, and second, because the statute shields them from any liability arising from their compliance with a § 215 order. See 50 U.S.C. § 1861(e). Any interests that they do have are distinct from those of their customers. The telephone service providers' primary interest would be the expense or burden of complying with the orders; only the customers have a direct interest in the privacy of information revealed in their telephone records.

Indeed, courts since Block have interpreted this factor – whether Congress has extended a cause of action to a party whose interests are aligned with those of a party seeking to sue – as critical to the heavily fact-bound Block decision.

The D.C. Circuit has noted that "some discussion in Block . . . sweep[s] broadly" but has concluded that, for example, the AMAA does not preclude milk *producers* (as opposed to *consumers*) from obtaining judicial review of market orders, in part because "[u]nlike the consumers whose interests were coextensive with those of handlers in Block, the producers are the only party with an interest in ensuring that the price paid them is not reduced by too large a[n amount] paid to handlers." Ark. Dairy Coop. Ass'n v. U.S. Dep't of Agric., 573 F.3d 815, 823 (D.C. Cir. 2009) (internal citation omitted). In other words, whether a party with aligned interests can obtain judicial review is an important consideration in interpreting and applying Block.

(3) Legislative History

Finally, the legislative history of the provision for challenging § 215 orders further supports appellants' argument that Congress did not intend to preclude targets of the orders from bringing suit. Appellants point out that the amendment to § 215 that provided for judicial review of § 215 orders in the FISC was passed in response to Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), vacated in part sub nom. Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006). At the same time it added the judicial review provision in § 215, Congress passed a

provision for judicial review in the context of National Security Letters ("NSLs") – a form of administrative subpoenas used to gather communications and records in national security matters. That subsection was added to address the court's concerns in Doe that 18 U.S.C. § 2709, pursuant to which NSLs are issued, "effectively bar[red] or substantially deter[red] any judicial challenge to the propriety of an NSL request." Doe, 334 F. Supp. 2d at 475. Congress's primary purpose in adopting both of these provisions was apparently to clarify that judicial review *was* available to recipients of NSLs and § 215 orders – not to *preclude* review at the behest of the targets of orders. In fact, in Doe, the government argued that the NSL statute already implicitly provided for judicial review. See id. at 492-93. The amendment, therefore, only "clarif[ied] that a FISA 215 order may be challenged and that a recipient of a 215 order may consult with the lawyer and the appropriate people necessary to respond to the order," H.R. Rep. No. 109-174, pt. 1, at 106 (statement of Chairman Sensenbrenner) – both concerns raised by the district court in Doe with respect to NSLs. The amendment was a clarification of the judicial review provision that already implicitly existed; in thus clarifying, it did not affirmatively take away a right to judicial review from another category of individuals not mentioned in the statute.

The government argues that Congress "specifically considered, and rejected, an amendment that would have allowed Section 215 orders to be challenged not only in the FISC, but also in district court." Appellees' Br. 29. But that is an oversimplification of the sequence of events relating to an amendment proposed by Representative Nadler. First, the proposed amendment encompassed more than the issue of judicial review. The amendment primarily proposed a more rigorous standard for obtaining orders under § 215 than existed at the time, and the bulk of the debate on the amendment concerned what degree of suspicion should be required for issuance of a § 215 order. See H.R. Rep. No. 109-174, pt. 1, at 128-32, 135 (2005). Second, the amendment proposed judicial review in a district court by the *recipients* of § 215 orders – a category of persons already granted an avenue of review under § 215, through the FISC process. Id. at 128, 134. It did not address – again, presumably because Congress did not have reason to consider the question at that point – whether a person whose records were seized as a result of such an order would be able, upon learning of the order, to challenge it in district court. Indeed, Representative Nadler specifically noted that his amendment did not grant judicial review at the behest of the "target" of a § 215 order because such a target "doesn't know about" the

order. See id. at 128 (statement of Rep. Nadler) ("It doesn't give the target of the order the ability to go to court. He doesn't know about it."); id. at 134 (statement of Rep. Nadler) ("[T]he fact is that . . . the target of the investigation never hears about this.").

As Justice Scalia has reminded us, moreover, we should exercise caution in relying on this type of legislative history in attempting to discern Congress's intent, because it is so often "impossible to discern what the Members of Congress intended except to the extent that intent is manifested in the *only* remnant of 'history' that bears the unanimous endorsement of the majority in each House: the text of the enrolled bill that became law." Graham County Soil & Water Conservation Dist. v. United States ex rel. Wilson, 559 U.S. 280, 302 (2010) (Scalia, J., concurring) (emphasis in original). Congress's rejection of the Nadler amendment cannot reliably be interpreted as a specific rejection of the opportunity for a § 215 target to obtain judicial review, under the APA or otherwise.

Finally, the government argues that Congress must have intended to preclude judicial review of § 215 orders, because if any customer of a company that receives a § 215 order may challenge such an order, lawsuits could be filed

by a vast number of potential plaintiffs, thus "severely disrupt[ing] . . . the sensitive field of intelligence gathering for counter-terrorism efforts." Appellees' Br. 30 (internal quotation marks omitted).

That argument, however, depends on the government's argument on the merits that bulk metadata collection was contemplated by Congress and authorized by § 215. The risk of massive numbers of lawsuits challenging the same orders, and thus risking inconsistent outcomes and confusion about the legality of the program, occurs only in connection with the existence of orders authorizing the collection of data from millions of people. Orders targeting limited numbers of persons under investigation could be challenged only by the individuals targeted – who, it was expected, would never learn of the orders in the first place. It is only in connection with the government's expansive *use* of § 215 (which, as will be seen below, was not contemplated by Congress) that these risks would create concern.

In any event, restricting judicial review of the legality of § 215 orders under the statute itself would do little to eliminate the specter of duplicative lawsuits challenging orders like the one at issue here. The government does not contend that those whose records are collected pursuant to § 215, assuming they have

established standing, are somehow precluded from bringing constitutional challenges to those orders. The government would thus attribute to Congress a preclusion of statutory challenges that would not eliminate the supposed dangers of multiplicative lawsuits, while channeling those lawsuits toward constitutional issues.

Such an outcome would be anomalous. It would fly in the face of the doctrine of constitutional avoidance, which "allows courts to *avoid* the decision of constitutional questions" by providing "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." Clark v. Martinez, 543 U.S. 371, 381 (2005) (emphasis in original). In contrast, the approach proffered by the government would preclude lawsuits challenging the legality of § 215 on statutory grounds, while leaving open the path to review of § 215 under the Constitution. While constitutional avoidance is a judicial doctrine, the principle should have considerable appeal to Congress: it would seem odd that Congress would preclude challenges to executive actions that allegedly violate Congress's own commands, and thereby channel the complaints of those aggrieved by such actions into constitutional

challenges that threaten Congress's own authority. There may be arguments in favor of such an unlikely scheme, but it cannot be said that any such reasons are so patent and indisputable that Congress can be assumed, in the face of the strong presumption in favor of APA review, to have adopted them without having said a word about them.

B. Section 2712 and Implied Preclusion

The other potentially relevant exception to the APA's waiver of sovereign immunity looks to whether "any *other* statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702 (emphasis added). The government urges that 18 U.S.C. § 2712, passed in the same statute that contained § 215, is just such a statute, granting as it does a private right of action for money damages against the United States for violations of the Wiretap Act, the Stored Communications Act, and three particular FISA provisions that concern electronic surveillance, physical searches, and pen registers or trap and trace devices (but not § 215). See 18 U.S.C. § 2712(a); see also 50 U.S.C. §§ 1806(a), 1825(a), 1845(a). Section 2712 withdrew the general right to sue the United States under the Wiretap Act and the Stored Communications Act at the same time it added a right of action for money damages. Importantly, it also stated that

"[a]ny action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section." 18 U.S.C. § 2712(d). According to the government, such provisions demonstrate that, where Congress did intend to allow a private right of action for violations of FISA, it did so expressly.

That the provision extending a right of action makes no mention of § 215, however, supports appellants' argument, not the government's. To be sure, "[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy . . . to be exclusive, that is the end of the matter; the APA does not undo the judgment." Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak, 132 S. Ct. 2199, 2205 (2012) (second alteration in original) (internal quotation marks omitted). But § 2712 does not deal "in particularity" with § 215. Instead, the government would have us conclude "that in authorizing one person to bring one kind of suit seeking one form of relief, Congress barred another person from bringing another kind of suit seeking another form of relief." Id. at 2209. Section 2712 makes no mention whatsoever of claims under § 215, either to permit them or to preclude them, and, as the Supreme Court stated in Patchak, "[w]e have never held, and see no cause to

hold here, that some general similarity of subject matter can alone trigger a remedial statute's preclusive effect." Id. The "exclusive remedy" provision applies only to claims within the purview of the remedial section, which does not cover all of FISA but rather specifies those FISA provisions to which it applies. Had Congress intended § 2712's exclusive right of action (and its preclusion of other remedies) to extend to § 215, it is fair to assume that it would have also enumerated that section – particularly considering the fact that both provisions were passed in the same statute.

Section 2712, moreover, *explicitly* withdraws the right to challenge the specific government actions taken under specific authorization, in connection with *extending* an explicit cause of action for monetary damages in connection with such actions. First, § 2712 shows that the Congress that enacted the PATRIOT Act understood very well how to withdraw the right to sue under the APA, and to create an exclusive remedy, when it wished to do so. Second, § 2712 manifestly does not create a cause of action for damages for violations of § 215, as it does with respect to those statutes of which it does preclude review under the APA.

Section 2712, therefore, does not preclude appellants' suit here. Nor do the two statutes, when viewed in combination, evince an intent of Congress to preclude suits by targets of § 215 orders.

C. Summary

In short, the government relies on bits and shards of inapplicable statutes, inconclusive legislative history, and inferences from silence in an effort to find an implied revocation of the APA's authorization of challenges to government actions. That is not enough to overcome the strong presumption of the general command of the APA against such implied preclusion. Congress, of course, has the ability to limit the remedies available under the APA; it has only to say so. But it has said no such thing here. We should be cautious in inferring legislative action from legislative inaction, or inferring a Congressional command from Congressional silence. At most, the evidence cited by the government suggests that Congress assumed, in light of the expectation of secrecy, that persons whose information was targeted by a § 215 order would rarely even know of such orders, and therefore that judicial review at the behest of such persons was a non-issue. But such an assumption is a far cry from an unexpressed intention to

withdraw rights granted in a generally applicable, explicit statute such as the APA.

Accordingly, we disagree with the district court insofar as it held that appellants here are precluded from bringing suit against the government, and hold that appellants have a right of action under the APA. We therefore proceed to the merits of the case.

III. Statutory Authorization

Although appellants vigorously argue that the telephone metadata program violates their rights under the Fourth Amendment to the Constitution, and therefore cannot be authorized by either the Executive or the Legislative Branch of government, or by both acting together, their initial argument is that the program simply has not been authorized by the legislation on which the government relies for the issuance of the orders to service providers to collect and turn over the metadata at issue. We naturally turn first to that argument.

Section 215 clearly sweeps broadly in an effort to provide the government with essential tools to investigate and forestall acts of terrorism. The statute permits the government to apply for "an order requiring the production of *any tangible things* . . . for an investigation . . . to protect against international

terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1) (emphasis added). A § 215 order may require the production of anything that "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation" or any other court order. Id. § 1861(c)(2)(D).

While the *types* of "tangible things" subject to such an order would appear essentially unlimited, such "things" may only be produced upon a specified factual showing by the government. To obtain a § 215 order, the government must provide the FISC with "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted [under guidelines approved by the Attorney General]." Id. § 1861(b)(2)(A); see id. § 1861(a)(2) (requiring that investigations making use of such orders be conducted under guidelines approved by the Attorney General). The basic requirements for metadata collection under § 215, then, are simply that the records be *relevant* to an *authorized investigation* (other than a threat assessment).

For all the complexity of the statutory framework, the parties' respective positions are relatively simple and straightforward. The government emphasizes that "relevance" is an extremely generous standard, particularly in the context of

the grand jury investigations to which the statute analogizes orders under § 215. Appellants argue that relevance is not an unlimited concept, and that the government's own use (or non-use) of the records obtained demonstrates that most of the records sought are not relevant to any particular investigation; the government does not seek the records, as is usual in a grand jury investigation, so as to review them in search of evidence bearing on a particular subject, but rather seeks the records to create a vast data bank, to be kept in reserve and queried if and when some particular set of records might be relevant to a particular investigation.

Echoing the district court's statement that "'[r]elevance' has a broad legal meaning," 959 F. Supp. 2d at 746, the government argues that the telephone metadata program comfortably meets the requisite standard. The government likens the relevance standard intended by Congress to the standard of relevance for grand jury and administrative subpoenas, and, to some extent, for civil discovery.

Both the language of the statute and the legislative history support the grand jury analogy. During the 2006 reauthorization debate, Senator Kyl recalled that, in passing the PATRIOT Act shortly after September 11, Congress had

realized that "it was time to apply to terrorism many of the same kinds of techniques in law enforcement authorities that we already deemed very useful in investigating other kinds of crimes. Our idea was, if it is good enough to investigate money laundering or drug dealing, for example, we sure ought to use those same kinds of techniques to fight terrorists." 152 Cong. Rec. S1607 (daily ed. Mar. 2, 2006) (statement of Sen. Kyl). He also remarked that "[r]elevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders." Id. at S1606. And it is well established that "where Congress borrows terms of art . . . , it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed." Morissette v. United States, 342 U.S. 246, 250 (1952).

So much, indeed, seems to us unexceptionable. In adopting § 215, Congress intended to give the government, on the approval of the FISC, broad-ranging investigative powers analogous to those traditionally used in connection with grand jury investigations into possible criminal behavior.

The government then points out that, under the accepted standard of relevance in the context of grand jury subpoenas, "courts have authorized discovery of large volumes of information where the requester seeks to identify within that volume smaller amounts of information that could directly bear on the matter." Appellees' Br. 31. The government asks us to conclude that it is "eminently reasonable to believe that Section 215 bulk telephony metadata is relevant to counterterrorism investigations." Id. at 32. Appellants, however, dispute that metadata from every phone call with a party in the United States, over a period of years and years, can be considered "relevant to an authorized investigation," by any definition of the term.

The very terms in which this litigation has been conducted by both sides suggest that the matter is not as routine as the government's argument suggests. Normally, the question of whether records demanded by a subpoena or other court order are "relevant" to a proceeding is raised in the context of a motion to quash a subpoena. The grand jury undertakes to investigate a particular subject matter to determine whether there is probable cause to believe crimes have been committed, and seeks by subpoena records that might contain evidence that will

help in making that determination.[4] Given the wide investigative scope of a grand jury, the standard is easy to meet, but the determination of relevance is constrained by the subject of the investigation. In resolving a motion to quash, a court compares the records demanded by the particular subpoena with the subject matter of the investigation, however broadly defined.

Here, however, the parties have not undertaken to debate whether the records required by the orders in question are relevant to any particular inquiry. The records demanded are all-encompassing; the government does not even suggest that all of the records sought, or even necessarily any of them, are relevant to any specific defined inquiry. Rather, the parties ask the Court to decide whether § 215 authorizes the "creation of a historical repository of information that bulk aggregation of the metadata allows," Appellees' Br. 32, because bulk collection to create such a repository is "necessary to the application

[4] Although subpoenas may be used in aid of other court proceedings, we take the grand jury as our example because the powers of the grand jury are particularly wide-ranging, and the standard of relevance or materiality of information sought is much more relaxed than, for example, in a trial, where to be relevant evidence must tend to make a fact "of consequence in determining the action," Fed. R. Evid. 401(b), "more or less probable than it would be without the evidence," id. 401(a).

of certain analytic techniques," Appellants' Br. 23. That is not the language in which grand jury subpoenas are traditionally discussed.

Thus, the government takes the position that the metadata collected – a vast amount of which does not contain directly "relevant" information, as the government concedes – are nevertheless "relevant" because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant.[5] We agree with appellants that such an expansive concept of "relevance" is unprecedented and unwarranted.

The statutes to which the government points have never been interpreted to authorize anything approaching the breadth of the sweeping surveillance at issue here.[6] The government admitted below that the case law in analogous

---

[5] Section 215 lists three factors that would render a tangible thing sought "presumptively relevant" to an authorized investigation, see 50 U.S.C. § 1861(b)(2)(A), but the records of ordinary telephone company customers' phone calls do not fall within any of those descriptions.

[6] A recently disclosed, now discontinued program under which the Drug Enforcement Administration utilized administrative subpoenas obtained pursuant to 21 U.S.C. § 876 to collect and maintain a telephone metadata database may have demanded an interpretation approaching the breadth of the government's interpretation of similar language here. See ECF No. 159 (Appellants' Fed. R. App. P. 28(j) letter); ECF No. 161 (Appellees' Fed. R. App. P.

contexts "d[id] not involve data acquisition on the scale of the telephony metadata collection." ACLU v. Clapper, No. 13 Civ. 3994 (S.D.N.Y. Aug. 26, 2013), ECF No. 33 (Mem. of Law of Defs. in Supp. of Mot. to Dismiss) at 24. That concession is well taken. As noted above, if the orders challenged by appellants do not require the collection of metadata regarding every telephone call made or received in the United States (a point asserted by appellants and at least nominally contested by the government), they appear to come very close to doing so. The sheer volume of information sought is staggering; while search warrants and subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here.

Moreover, the distinction is not merely one of quantity – however vast the quantitative difference – but also of quality. Search warrants and document subpoenas typically seek the records of a particular individual or corporation

---

28(j) letter). That program, which, according to both parties, has been discontinued, is not being challenged here, and we therefore need not opine as to whether the language of the statute pursuant to which the metadata were collected authorized that program.

under investigation, and cover particular time periods when the events under investigation occurred. The orders at issue here contain no such limits. The metadata concerning *every* telephone call made or received in the United States using the services of the recipient service provider are demanded, for an indefinite period extending into the future. The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with the subjects – they extend to every record that exists, and indeed to records that do not *yet* exist, as they impose a continuing obligation on the recipient of the subpoena to provide such records on an ongoing basis as they are created. The government can point to no grand jury subpoena that is remotely comparable to the real-time data collection undertaken under this program.

Nevertheless, the government emphasizes the permissive standards applied to subpoenas, noting that, at least in the context of grand jury subpoenas, motions to quash on relevancy grounds are "denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enters., Inc., 498 U.S. 292, 301

(1991). That is because such subpoenas "are customarily employed to gather information and make it available to the investigative team of agents and prosecutors so that it can be digested and sifted for pertinent matter" and are therefore "often drawn broadly, sweeping up both documents that may prove decisive and documents that turn out not to be." United States v. Triumph Capital Grp., 544 F.3d 149, 168 (2d Cir. 2008).

In that vein, the government points to cases in which courts have upheld subpoenas for broad categories of information and for "large-scale collection[] of information." Appellees' Br. 33 (internal quotation marks omitted). For example, in In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301 (8th Cir. 1987), the Eighth Circuit denied Western Union's motion to quash a subpoena that requested production by Western Union's primary wire service agent in Kansas City of all money order applications for amounts over $1,000 over a more than two-year period, and of a report summarizing all wire transactions it conducted over an approximate one-year period. Despite Western Union's argument that the subpoena would sweep in "records involving hundreds of innocent people," the court stated that grand juries are not necessarily prohibited from engaging in "dragnet operation[s]." Id. at 305 (internal quotation marks

omitted). In In re Subpoena Duces Tecum, 228 F.3d 341 (4th Cir. 2000), the Fourth Circuit also denied a motion to quash a subpoena issued to a doctor requiring production of, inter alia, all patient records and documentation concerning patients whose services were billed to Medicare, Medicaid, and a number of insurance companies, including the patients' complete medical files, their billing records, office appointment books, sign-in sheets, and telephone messages, over a period of at least seven years. That court held that the subpoena did not sweep too broadly, despite the high volume of documents it demanded, in part because of the scope of the fraud being investigated and the size of the doctor's practice. Id. at 350-51; see also Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946) ("[R]elevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry.").

But broad as those subpoenas were, the cases cited by the government only highlight the difference between the investigative demands at issue in those cases and the ones at issue here. Both of those examples, and all examples of which we are aware, are bounded either by the facts of the investigation or by a finite time limitation. The telephone metadata program requires that the phone companies

turn over records on an "ongoing daily basis" – with no foreseeable end point, no requirement of relevance to any particular set of facts, and no limitations as to subject matter or individuals covered.[7] Even in the Eighth Circuit case that the government cites, moreover, although it upheld the subpoena at issue, the Eighth Circuit suggested that the district court "consider the extent to which the government would be able to identify in advance . . . patterns or characteristics that would raise suspicion . . . designed to focus on illegal activity without taking in an unnecessary amount of irrelevant material." In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d at 305-06. Courts have typically looked to constrain even grand jury subpoenas to a standard of reasonableness related to a defined investigative scope; we have found excessively broad a subpoena requiring production of all of an accountant's files within a mere three filing

[7] Drawing an analogy again to the context of administrative subpoenas, we note too that courts are "more reluctant to enforce subpoenas when agencies have sought records of third parties who were not targets of the agency's investigation." In re McVane, 44 F.3d 1127, 1137 (2d Cir. 1995). The overwhelming bulk of the metadata collected by the telephone metadata program, as the government itself concedes, concerns "third parties" in that sense of the word – individuals who are not targets of an investigation or suspected of engaging in any crime whatsoever, and who are not even suspected of having any contacts with any such targets or suspects. Their records are sought solely to build a repository for the future application of the investigative techniques upon which the program relies.

cabinets, "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period," because it swept in papers that there was no reason to believe were relevant. In re Horowitz, 482 F.2d 72, 79 (2d Cir. 1973). We therefore limited the subpoena's time period absent the government's making a minimal showing of relevance. Id. at 79-80.

To the extent that § 215 was intended to give the government, as Senator Kyl proposed, the "same kinds of techniques to fight terrorists" that it has available to fight ordinary crimes such as "money laundering or drug dealing," 152 Cong. Rec. S1607 (daily ed. Mar. 2, 2006) (statement of Sen. Kyl), the analogy is not helpful to the government's position here. The techniques traditionally used to combat such ordinary crimes have not included the collection, via grand jury subpoena, of a vast trove of records of metadata concerning the financial transactions or telephone calls of ordinary Americans to be held in reserve in a data bank, to be searched if and when at some hypothetical future time the records might become relevant to a criminal investigation.

The government's emphasis on the potential breadth of the term "relevant," moreover, ignores other portions of the text of § 215. "Relevance"

does not exist in the abstract; something is "relevant" or not in relation to a particular subject. Thus, an item relevant to a grand jury investigation may not be relevant at trial. In keeping with this usage, § 215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents "relevant to an authorized *investigation*." The government has not attempted to identify to what particular "authorized investigation" the bulk metadata of virtually all Americans' phone calls are relevant. Throughout its briefing, the government refers to the records collected under the telephone metadata program as relevant to "counterterrorism investigations," without identifying any specific investigations to which such bulk collection is relevant. See, e.g., Appellees' Br. 32, 33, 34.[8] The FISC orders, too, refer only to "authorized investigations (other than threat assessments) being

[8] While the government purports to have provided "examples" of "specific counter-terrorism investigations," see Appellees' Br. 33, citing Joint App'x 254-55, those examples serve only as instances in which the metadata already collected in bulk were able to be queried and resulted in identification of a previously unknown contact of known terrorists. The government does not contend that most of the metadata already collected were relevant to any of those particular investigations, let alone that it was able to so demonstrate prior to the collection of those metadata.

conducted by the FBI . . . to protect against international terrorism," see, e.g., 2006 Primary Order at 2; Joint App'x 127, 317, merely echoing the language of the statute. The PCLOB report explains that the government's practice is to list in § 215 applications multiple terrorist organizations, and to declare that the records being sought are relevant to the investigations of all of those groups. PCLOB Report 59. As the report puts it, that practice is "little different, in practical terms, from simply declaring that they are relevant to counterterrorism in general. . . . At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations." Id. at 59-60. Put another way, the government effectively argues that there is only one enormous "anti-terrorism" investigation, and that any records that might ever be of use in developing any aspect of that investigation are relevant to the overall counterterrorism effort.

The government's approach essentially reads the "authorized investigation" language out of the statute. Indeed, the government's information-gathering under the telephone metadata program is inconsistent with the very concept of an "investigation." To "investigate" something, according to the Oxford English Dictionary, is "[t]o search or inquire into; to

examine (a matter) systematically or in detail; to make an inquiry or examination into."[9] 8 Oxford English Dictionary 47 (2d ed. 2001). Section 215's language thus contemplates the specificity of a particular investigation – not the general counterterrorism intelligence efforts of the United States government. But the records in question here are not sought, at least in the first instance, because the government plans to examine them in connection with a "systematic examination" of anything at all; the records are simply stored and kept in reserve until such time as some particular investigation, in the sense in which that word is traditionally used in connection with legislative, administrative, or criminal inquiries, is undertaken. Only at that point are any of the stored records examined. The records sought are not even asserted to be relevant to any on-going "systematic examination" of any particular suspect, incident, or group; they are relevant, in the government's view, because there might at some future point be a need or desire to search them in connection with a hypothetical future inquiry.

[9] The noun form "investigation" is similarly defined as "[t]he action of investigating; the making of a search or inquiry; systematic examination; careful and minute research." 8 Oxford English Dictionary 47 (2d ed. 2001).

The government's approach also reads out of the statute another important textual limitation on its power under § 215. Section 215 permits an order to produce records to issue when the government shows that the records are "relevant to an authorized investigation *(other than a threat assessment)*." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). The legislative history tells us little or nothing about the meaning of "threat assessment." The Attorney General's Guidelines for Domestic FBI Operations, however, tell us somewhat more. The Guidelines divide the category of "investigations and intelligence gathering" into three subclasses: assessments, predicated investigations (both preliminary and full), and enterprise investigations. See Attorney General's Guidelines for Domestic FBI Operations 16-18 (2008), https://www.ignet.gov/sites/default/files/files/invprg1211appg1.pdf. Assessments are distinguished from investigations in that they may be initiated without any factual predication. Id. at 17. The Guidelines cite the objective of preventing the commission of terrorist acts against the nation as an example of a proper assessment objective, stating that the FBI "must proactively draw on available sources of information to identify terrorist threats and activities." Id. The methods used in assessments are "generally those of relatively low

intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public." Id. at 17-18. Because of that low level of intrusiveness, the Guidelines do not require supervisory approval for assessments, although FBI policy may require it in particular cases, depending on the assessment's purpose and the methods being used. Id. at 18.

The FBI Domestic Investigations and Operations Guide elaborates on this scheme. It too provides that threat assessments "do not require a particular factual predication but do require an authorized purpose and clearly defined objective(s). Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence." FBI Domestic Investigations and Operations Guide § 5.1 (2011), http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version/fbi-domestic-investigations-and-operations-guide-diog-october-15-2011-part-01-of-03/view. Although no specific factual predicate is required, the

Guide makes clear that assessments cannot be based on "arbitrary or groundless speculation." Id. It adds:

> Although difficult to define, "no particular factual predication" is less than "information or allegation" as required for the initiation of a preliminary investigation (PI). For example, an Assessment may be conducted when: (i) there is reason to collect information or facts to determine whether there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the Assessment on the one hand and the information sought and the proposed means to obtain that information on the other.

Id.

In limiting the use of § 215 to "investigations" rather than "threat assessments," then, Congress clearly meant to *prevent* § 215 orders from being issued where the FBI, without any particular, defined information that would permit the initiation of even a preliminary investigation, sought to conduct an inquiry in order to identify a potential threat in advance. The telephone metadata program, however, and the orders sought in furtherance of it, are even more remote from a concrete investigation than the threat assessments that – however important they undoubtedly are in maintaining an alertness to possible threats to national security – Congress found not to warrant the use of § 215

orders. After all, when conducting a threat assessment, FBI agents must have both a reason to conduct the inquiry and an articulable connection between the particular inquiry being made and the information being sought. The telephone metadata program, by contrast, seeks to compile data in advance of the need to conduct any inquiry (or even to examine the data), and is based on no evidence of any current connection between the data being sought and any existing inquiry.

We agree with the PCLOB, which concluded that the government's rationale for the "relevance" of the bulk collection of telephone metadata "undermines" the prohibition on using § 215 orders for threat assessments:

> [Section 215] provides that records cannot be obtained for a "threat assessment," meaning those FBI investigatory activities that "do not require a particular factual predicate." By excluding threat assessments from the types of investigations that can justify an order, Congress directed that Section 215 not be used to facilitate the broad and comparatively untethered investigatory probing that is characteristic of such assessments. But by collecting the nation's calling records *en masse*, under an expansive theory of their relevance to multiple investigations, the NSA's program undercuts one of the functions of the "threat assessment" exclusion: ensuring that records are not acquired by the government without some reason to suspect a connection between those records and a specific, predicated terrorism investigation. While the rules

> governing the program limit the *use* of telephone records to searches that are prompted by a specific investigation, the relevance requirement in Section 215 restricts the *acquisition* of records by the government.

PCLOB Report 60 (emphases in original) (footnote omitted).[10]

The interpretation urged by the government would require a drastic expansion of the term "relevance," not only with respect to § 215, but also as that term is construed for purposes of subpoenas, and of a number of national security-related statutes, to sweep further than those statutes have ever been thought to reach. For example, the same language is used in 18 U.S.C. § 2709(b)(1) and 20 U.S.C. § 1232g(j)(1)(A), which authorize, respectively, the compelled production of telephone toll-billing and educational records relevant to authorized investigations related to terrorism. There is no

[10] The government also argues that, aside from their relevance to the subject matter of counterterrorism, the telephone metadata records are relevant to authorized investigations in that they are necessary for the government to apply certain investigative techniques – here, searching based on "selectors" through the government's metadata repository. That argument proves too much. If information can be deemed relevant solely because of its necessity to a particular process that the government has chosen to employ, regardless of its subject matter, then so long as "the government develops an effective means of searching through *everything* in order to find *something*, . . . *everything* becomes relevant to its investigations" – and the government's "technological capacity to ingest information and sift through it efficiently" would be the only limit to what is relevant. PCLOB Report 62 (emphases in original).

evidence that Congress intended for those statutes to authorize the bulk collection of every American's toll-billing or educational records and to aggregate them into a database — yet it used nearly identical language in drafting them to that used in § 215. The interpretation that the government asks us to adopt defies any limiting principle. The same rationale that it proffers for the "relevance" of telephone metadata cannot be cabined to such data, and applies equally well to other sets of records. If the government is correct, it could use § 215 to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and social media information) relating to all Americans.

Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language. There is no evidence of such a debate in the legislative history of § 215, and the

language of the statute, on its face, is not naturally read as permitting investigative agencies, on the approval of the FISC, to do any more than obtain the sorts of information routinely acquired in the course of criminal investigations of "money laundering [and] drug dealing."

We conclude that to allow the government to collect phone records only because they may become relevant to a possible authorized investigation in the future fails even the permissive "relevance" test. Just as "the grand jury's subpoena power is not unlimited," United States v. Calandra, 414 U.S. 338, 346 (1974), § 215's power cannot be interpreted in a way that defies any meaningful limit. Put another way, we agree with appellants that the government's argument is "irreconcilable with the statute's plain text." Appellants' Br. 26. Such a monumental shift in our approach to combating terrorism requires a clearer signal from Congress than a recycling of oft-used language long held in similar contexts to mean something far narrower. "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions — it does not . . . hide elephants in mouseholes." Whitman v. Am. Trucking Ass'ns., 531 U.S. 457, 468 (2001). The language of § 215 is decidedly too ordinary for what the government would have us believe is such an

extraordinary departure from any accepted understanding of the term "relevant to an authorized investigation."

Finally, as it did with respect to the question of judicial review, the government again resorts to the claim that if Congress did not *explicitly* adopt the rule for which it argues, it did so *implicitly*. Here, the government argues that Congress has ratified the FISC's interpretation of § 215, and thus the telephone metadata program, by reauthorizing § 215 in 2010 and 2011. We reject that argument.

First, the theory of congressional ratification of judicial interpretations of a statute by reenactment cannot overcome the plain meaning of a statute. "Where the law is plain, subsequent reenactment does not constitute an adoption of a previous administrative construction." Demarest v. Manspeaker, 498 U.S. 184, 603 (1991).

Second, although "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change," Lorillard v. Pons, 434 U.S. 575, 580 (1978), there are limits to that presumption — particularly where, as here, knowledge of the program was intentionally kept to a minimum, both within Congress and among

the public. We have said that, at least in the case of an administrative interpretation of a statute, for the doctrine of legislative ratification to apply, we must first "ascertain whether Congress has spoken clearly enough to constitute acceptance and approval of an administrative interpretation. Mere reenactment is insufficient." Isaacs v. Bowen, 865 F.2d 468, 473 (2d Cir. 1989). In Atkins v. Parker, the Supreme Court applied the doctrine of legislative ratification where "Congress was . . . well aware of, and legislated on the basis of, . . . contemporaneous administrative practice," concluding that it therefore "must be presumed to have intended to maintain that practice absent some clear indication to the contrary." 472 U.S. 115, 140 (1985). In contrast, in a situation in which "there [wa]s nothing to indicate that [the interpretation of a regulation] was ever called to the attention of Congress," and the statute's reenactment "was not accompanied by any congressional discussion which throws light on its intended scope," the Court has "consider[ed] the . . . re-enactment to be without significance." United States v. Calamaro, 354 U.S. 351, 359 (1957); see also Comm'r v. Glenshaw Glass Co., 348 U.S. 426, 431 (1955) ("Re-enactment [of a statute] – particularly without the slightest affirmative indication that Congress ever had [a particular] decision before it – is an unreliable indicium at best.").

Third, as the above precedents suggest, the public nature of an interpretation plays an important role in applying the doctrine of legislative ratification. The Supreme Court has stated that "[w]here an agency's statutory construction has been fully brought to the attention of the public and the Congress, and the latter has not sought to alter that interpretation although it has amended the statute in other respects, then presumably the legislative intent has been correctly discerned." North Haven Bd. of Educ. v. Bell, 456 U.S. 512, 535 (1982) (internal quotation marks omitted); see also United States v. Chestman, 947 F.2d 551, 560 (2d Cir. 1991). Congressional inaction is already a tenuous basis upon which to infer much at all, even where a court's or agency's interpretation is fully accessible to the public and to all members of Congress, who can discuss and debate the matter among themselves and with their constituents. But here, far from the ordinarily publicly accessible judicial or administrative opinions that the presumption contemplates, no FISC opinions authorizing the program were made public prior to 2013 — well after the two occasions of reauthorization upon which the government relies, and despite the fact that the FISC first authorized the program in 2006.

Congress cannot reasonably be said to have ratified a program of which many members of Congress – and all members of the public – were not aware. In 2010, the Senate and House Intelligence Committees requested that the Executive Branch provide all members of Congress access to information about the program before the reauthorization vote. In response, the Executive Branch provided the Intelligence Committee chairs with a classified paper on the program, which was then made available to members of Congress. That availability, however, was limited in a number of ways. First, the briefing papers could only be viewed in secure locations, for a limited time period and under a number of restrictions. See Joint App'x 148-165. The government does not dispute appellants' assertion that members of Congress could not bring staff with them when they went to read the briefing papers, nor discuss the program with their staff. And, of course, no public debate on the program took place. In 2011, briefing papers were also provided to the Intelligence Committees, but only the Senate Committee shared the papers with other members of that body who were not committee members. The House Intelligence Committee did not share the papers at all with non-members, leaving the non-committee Representatives in

the dark as to the program. See generally id. at 170-73; see also Clapper, 959 F. Supp. 2d at 745.

To be sure, the government is correct that whether a particular interpretation was legislatively ratified ordinarily should not depend on the "number of legislators with actual knowledge of the government's interpretation." Appellees' Br. 36. We do not insist, in the ordinary case, on evidence that members of Congress actually read and understood administrative or judicial decisions interpreting a statute to apply the doctrine of ratification. But this is far from the ordinary case. In the ordinary case in which we apply the Lorillard presumption, the administrative or judicial interpretation argued to have been ratified by Congress was available to the public in published sources. Concerned citizens and interest groups had every opportunity to bring interpretations that they believed were incorrect or undesirable to the attention of their representatives in the House and Senate, and to lobby for legislation rejecting those interpretations. To the extent that some members of Congress were unaware of the details of those interpretations, their ignorance itself very likely reflected the absence of any particular controversy surrounding them.

In sharp contrast, the telephone metadata program was (for understandable reasons) shrouded in the secrecy applicable to classified information, and only a limited subset of members of Congress had a comprehensive understanding of the program or of its purported legal bases. There was certainly no opportunity for broad discussion in the Congress or among the public of whether the FISC's interpretation of § 215 was correct.[11] Finding the government's interpretation of the statute to have been "legislatively ratified" under these circumstances would ignore reality. Practically speaking, it is a far stretch to say that Congress was aware of the FISC's legal interpretation of § 215 when it reauthorized the statute in 2010 and 2011. We therefore cannot accept the argument that Congress, by reauthorizing § 215 without change in 2010 and 2011, thereby legislatively ratified the interpretation of § 215 urged by the government. The widespread controversy that developed, in and out of Congress, upon the public disclosure of the program makes clear that this is not a

[11] Indeed, the discrepancy between the conclusion we reach herein and that reached by the FISC may, at least in part, be accounted for by our having received the benefit of an adversarial presentation of the issues. See post at pp. 6, 11 (Sack, J., concurring).

situation in which Congress quietly but knowingly adopted the FISC's interpretation of § 215 because there was no real opposition to that interpretation.

For all of the above reasons, we hold that the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program. We do so comfortably in the full understanding that if Congress chooses to authorize such a far-reaching and unprecedented program, it has every opportunity to do so, and to do so unambiguously. Until such time as it does so, however, we decline to deviate from widely accepted interpretations of well-established legal standards. We therefore disagree with the district court insofar as it held that appellants' statutory claims failed on the merits, and vacate its judgment dismissing the complaint.

IV. Constitutional Claims

In addition to arguing that the telephone metadata program is not authorized by § 215, appellants argue that, even if the program is authorized by statute, it violates their rights under the Fourth and First Amendments to the

Constitution. The Fourth Amendment claim, in particular, presents potentially vexing issues.[12]

Appellants contend that the seizure from their telephone service providers, and eventual search, of records of the metadata relating to their telephone communications violates their expectations of privacy under the Fourth Amendment in the absence of a search warrant based on probable cause to believe that evidence of criminal conduct will be found in the records. The government responds that the warrant and probable cause requirements of the Fourth Amendment are not implicated because appellants have no privacy rights in the records. This dispute touches an issue on which the Supreme Court's jurisprudence is in some turmoil.

---

[12] For that reason, we discuss infra some of the Fourth Amendment concerns that the program implicates. As to the First Amendment issues, appellants argue that the program infringes their First Amendment associational privacy and free speech rights, "substantially impair[ing]" those rights by "expos[ing] their telephonic associations to government monitoring and scrutiny." Appellants' Br. 53. They contend that the program must therefore survive "exacting scrutiny." Id. at 58. The government responds, as to the merits of appellants' First Amendment claim, that any such burdens are merely "incidental." Appellees' Br. 54. As noted infra, because we find that the telephone metadata program exceeds the bounds of what is authorized by § 215, we need not reach either constitutional issue, and we see no reason to discuss the First Amendment claims in greater depth.

In Katz v. United States, 389 U.S. 347 (1967), the Supreme Court departed from the property-based approach to the Fourth Amendment that had governed since Olmstead v. United States, 277 U.S. 438 (1928), which depended upon whether an actual physical trespass of property had occurred. As explained in Justice Harlan's concurring opinion, the Court held in Katz that a search occurs where "a person ha[s] exhibited an actual (subjective) expectation of privacy, and . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring).

The Supreme Court has also long held, however, that individuals have no "legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979); see, e.g., California v. Greenwood, 486 U.S. 35 (1988) (no objectively reasonable expectation of privacy in garbage exposed to the public by being placed on a sidewalk); United States v. Miller, 425 U.S. 435 (1976) (no legitimate expectation of privacy in bank records). In Smith v. Maryland, the Court applied that doctrine to uphold the constitutionality of installing a pen register at a telephone company's office that recorded the numbers dialed from a criminal suspect's home telephone. 442 U.S. at 737, 745-46. The Court held that the installation of the pen register was not a

search for Fourth Amendment purposes because, by placing calls, individuals expose the telephone numbers they dial to the telephone company and therefore "assume[] the risk that the company [may] reveal to police the numbers . . . dialed." Id. at 744. Similarly, it has long been commonplace for grand juries to subpoena an individual's telephone records from the individual's telephone service provider, in the absence of probable cause or a warrant issued by a judge. The acquisition of such records, it has been held, implicates no legitimate privacy interest of the subscriber, because the records are not his or hers alone. See, e.g., id. at 742-44; Miller, 425 U.S. at 443; Couch v. United States, 409 U.S. 322, 334-36 (1973). The subscriber cannot reasonably believe that the records are private, because he or she has voluntarily exposed the information contained in them to the telephone company, which uses them for its own business purpose of billing the subscriber.

The government argues, and the district court held, that this doctrine requires rejection of appellants' claim that the acquisition of telephone metadata (as opposed to the contents of communications) violates the Fourth Amendment, or even implicates its protections at all. Appellants respond that modern

technology requires revisitation of the underpinnings of the third-party records doctrine as applied to telephone metadata.

Appellants' argument invokes one of the most difficult issues in Fourth Amendment jurisprudence: the extent to which modern technology alters our traditional expectations of privacy. On the one hand, the very notion of an individual's expectation of privacy, considered in Katz a key component of the rights protected by the Fourth Amendment, may seem quaint in a world in which technology makes it possible for individuals and businesses (to say nothing of the government) to observe acts of individuals once regarded as protected from public view. On the other hand, rules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows.

Appellants point to the Supreme Court's decision in United States v. Jones, 132 S. Ct. 945 (2012), as exemplifying the kind of challenge to apparently established law that they seek to bring. Jones does not address telephone or other business records, but arose in the somewhat analogous context of physical surveillance. Prior to Jones, in United States v. Knotts, 460 U.S. 276 (1983), in a

ruling based in substantial part on the core notion that an individual has no expectation of privacy in what he exposes to the eyes of third parties, the Court held that a person has no expectation of privacy in his public movements, because he "voluntarily convey[s] to anyone who want[s] to look the fact that he [i]s traveling on particular roads in a particular direction, the fact of whatever stops he ma[kes], and the fact of his final destination." Id. at 281-82. The Court therefore ruled that, just as police agents may follow a suspect in public without a warrant or probable cause, the government's use of a beeper to follow a suspect without a warrant was constitutional; the beeper merely "augment[ed]" the officers' normal sensory faculties, but did nothing that an individual otherwise monitoring the suspect could not do without it. Id. at 282. The Court noted, however, in response to concern about the potential for twenty-four hour surveillance without judicial supervision, that "if . . . dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Id. at 284.

That opportunity came decades later, in Jones. In that case, the government had tracked an individual's location over the course of 28 days using

a GPS tracking device it had attached to his vehicle without first obtaining a warrant. 132 S. Ct. at 948. The D.C. Circuit held that, because an individual does not expose his location to the public over the course of an entire month, either actually or constructively, the proper framework from which to analyze the operation was not a variation on the third-party doctrine but instead Katz's reasonable expectation of privacy standard. United States v. Maynard, 615 F.3d 544, 555-63 (D.C. Cir. 2010), aff'd on other grounds sub nom. Jones, 132 S. Ct. 945. It held that the defendant's expectation of privacy had been violated, because the long-term surveillance revealed a "mosaic" of information in which individuals had privacy interests, even in the absence of a privacy interest in discrete pieces of such information. Id. at 562-63.

The Supreme Court affirmed the D.C. Circuit's opinion, but on different grounds. It held that the operation was a search entitled to Fourth Amendment protection because the attachment of the GPS device constituted a technical trespass on the defendant's vehicle. Jones, 132 S. Ct. at 949-53. The Court's majority opinion declined to reach the issue of whether the operation would have passed Katz's "reasonableness" test, id. at 954, or whether the third-party doctrine instead applied, id. at 952.

As appellants note, however, five of the Justices appeared to suggest that there might be a Fourth Amendment violation even without the technical trespass upon which the majority opinion relied. Four of the Justices argued that the Court should have applied the Katz "reasonableness" test, and that the surveillance would not survive that test. Id. at 957-58, 964 (Alito, J., concurring). Justice Sotomayor noted in another concurring opinion that "the majority opinion's trespassory test may provide little guidance" for certain modern-day surveillance techniques, for which physical trespass is often not necessary. Id. at 955 (Sotomayor, J., concurring). Consequently, she observed that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," noting that such an approach is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Id. at 957.

Appellants argue that the telephone metadata program provides an archetypal example of the kind of technologically advanced surveillance techniques that, they contend, require a revision of the third-party records doctrine. Metadata today, as applied to individual telephone subscribers,

particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls (and not merely, as in traditional criminal investigations, for a limited period connected to the investigation of a particular crime), permit something akin to the 24-hour surveillance that worried some of the Court in Jones. Moreover, the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a potential for invasions of privacy unimaginable in the past. Thus, appellants argue, the program cannot simply be sustained on the reasoning that permits the government to obtain, for a limited period of time as applied to persons suspected of wrongdoing, a simple record of the phone numbers contained in their service providers' billing records.

Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues. The seriousness of the constitutional concerns, however, has some bearing on what we hold today, and on the consequences of that holding.

We note first that whether Congress has considered and authorized a program such as this one is not irrelevant to its constitutionality. The endorsement of the Legislative Branch of government provides some degree of comfort in the face of concerns about the reasonableness of the government's assertions of the necessity of the data collection. Congress is better positioned than the courts to understand and balance the intricacies and competing concerns involved in protecting our national security, and to pass judgment on the value of the telephone metadata program as a counterterrorism tool. Moreover, the legislative process has considerable advantages in developing knowledge about the far-reaching technological advances that render today's surveillance methods drastically different from what has existed in the past, and in understanding the consequences of a world in which individuals can barely function without involuntarily creating metadata that can reveal a great deal of information about them. A congressional judgment as to what is "reasonable" under current circumstances would carry weight – at least with us, and, we assume, with the Supreme Court as well – in assessing whether the availability of information to telephone companies, banks, internet service providers, and the like, and the ability of the government to collect and process volumes of such data that would

previously have overwhelmed its capacity to make use of the information, render obsolete the third-party records doctrine or, conversely, reduce our expectations of privacy and make more intrusive techniques both expected and necessary to deal with new kinds of threats.

Finally, we are not unmindful that a full debate by Congress of the appropriateness of a program such as that now operated by the government may result in the approval of a program with greater safeguards for privacy, or with other limitations, that are not now in place and that could alter or even moot the issues presented by appellants.[13] In the last Congress, for example, a bill to authorize a modified version of the telephone metadata program, supported by the Administration, passed the House of Representatives; a similar bill failed in the Senate after a majority of senators – but not the required 60 to cut off debate – sought to bring the bill to a vote. See USA FREEDOM Act, H.R. 3361, 113th Cong. (2014); USA FREEDOM Act, S. 2685, 113th Cong. (2014). As noted above, more recently, on April 30, 2015, a modified version of the USA FREEDOM Act, which would limit the bulk metadata program in various ways, was passed by

[13] We note that, at oral argument, appellants' counsel indicated that the adoption of certain measures would lead at least these appellants to withdraw their constitutional challenges.

the House Judiciary Committee, see USA FREEDOM Act of 2015, H.R. 2048, 114th Cong. (2015), and a vote in that Chamber is expected later this month. An identical bill has been introduced in the Senate and referred to the Senate Judiciary Committee. See USA FREEDOM Act of 2015, S. 1123, 114th Cong. (2015).

We reiterate that, just as we do not here address the constitutionality of the program as it currently exists, we do not purport to express any view on the constitutionality of any alternative version of the program. The constitutional issues, however, are sufficiently daunting to remind us of the primary role that should be played by our elected representatives in deciding, explicitly and after full debate, whether such programs are appropriate and necessary. Ideally, such issues should be resolved by the courts only after such debate, with due respect for any conclusions reached by the coordinate branches of government.

V. Preliminary Injunction

Finally, we consider the district court's denial of appellants' motion for a preliminary injunction. A party seeking a preliminary injunction must either show that he is likely to succeed on the merits; that he is likely to suffer irreparable harm in the absence of preliminary relief; that the balance of equities

tips in his favor; and that an injunction is in the public interest, Winter v. NRDC, 555 U.S. 7, 20 (2008); or he may show irreparable harm and either a likelihood of success on the merits or "sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly toward the party requesting the preliminary relief," Christian Louboutin S.A. v. Yves Saint Laurent Am. Holdings, Inc., 696 F.3d 206, 215 (2d Cir. 2012) (internal quotation marks omitted).

Here, as is clear from our analysis above, the district court erred in certain respects on several issues of law critical to deciding the legality of the government's program. On a correct view of those issues, appellants have shown a likelihood – indeed, a certainty – of success on the merits of at least their statutory claims. Appellants argue that, because they have alleged a deprivation of constitutional rights, we should presume irreparable harm, and that the balance of equities tips in their favor, because the government does not have any legitimate interest in conducting unlawful surveillance.

At least at this point, however, we decline to conclude that a preliminary injunction is required, and leave it to the district court to reconsider, in the first instance, the propriety of preliminary relief in light of a correct understanding of

the governing law. We note that at the present time, § 215 is scheduled to expire in just several weeks. The government vigorously contends that the program is necessary for maintaining national security, which of course is a public interest of the highest order. Allowing the program to remain in place for a few weeks while Congress decides whether and under what conditions it should continue is a lesser intrusion on appellants' privacy than they faced at the time this litigation began. In light of the asserted national security interests at stake, we deem it prudent to pause to allow an opportunity for debate in Congress that may (or may not) profoundly alter the legal landscape.

Moreover, given the necessity of congressional action, the statutory issues on which we rest our decision could become moot (at least as far as the future of the telephone metadata program is concerned), and the constitutional issues appellants continue to press radically altered, by events that will occur in a short time frame. If Congress decides to authorize the collection of the data desired by the government under conditions identical to those now in place, the program will continue in the future under that authorization. There will be time then to address appellants' constitutional issues, which may be significantly altered by the findings made, and conclusions reached, by the political branches, and to

decide what if any relief appellants are entitled to based on our finding that the program as it has operated to date is unlawful. If Congress decides to institute a substantially modified program, the constitutional issues will certainly differ considerably from those currently raised. If Congress fails to reauthorize § 215 itself, or reenacts § 215 without expanding it to authorize the telephone metadata program, there will be no need for prospective relief, since the program will end, and once again there will be time to address what if any relief is required in terms of the data already acquired by the government. We believe that such issues will be best addressed in the first instance by the district court in due course.

CONCLUSION

This case serves as an example of the increasing complexity of balancing the paramount interest in protecting the security of our nation – a job in which, as the President has stated, "actions are second-guessed, success is unreported, and failure can be catastrophic," Remarks by the President on Review of Signals Intelligence – with the privacy interests of its citizens in a world where surveillance capabilities are vast and where it is difficult if not impossible to avoid exposing a wealth of information about oneself to those surveillance

mechanisms. Reconciling the clash of these values requires productive contribution from all three branches of government, each of which is uniquely suited to the task in its own way.

For the foregoing reasons, we conclude that the district court erred in ruling that § 215 authorizes the telephone metadata collection program, and instead hold that the telephone metadata program exceeds the scope of what Congress has authorized and therefore violates § 215. Accordingly, we VACATE the district court's judgment dismissing the complaint and REMAND the case to the district court for further proceedings consistent with this opinion.